Social Media Scams

A friend commented on your post or shared your picture and you see a notification from your app or an email arrives. You're excited to see who's interested in your content, so you click the link in the notification or email and bam! You download malware to your device. That's how quick it can happen. Just like in emails, the scammers entice you with something intriguing then direct you to click on their trap; and social media is no different. The only difference is the general public is less trained to watch for scams on social media than they are in noticing spam emails.

A common scam with **Facebook®** is posting a catchy image that looks like a video with the play button. When the viewer thinks they are clicking the play button, they are taken to another site that looks just like the social media's login page, with the same logos, color schemes, and content. The user then assumes they need to login again - when they're really giving their login credentials to the scammer! To take it a step further, the video shows up again after the user "logs in." After the user tries to view it again, they are asked to download the video. Yep, you guessed it! It's not a video that is being downloaded, rather, it's malware or adware, or both.

If phishing spam isn't coming fast and furiously enough for you, developers from security firms have created an automated spear phishing tool that snagged **Twitter®** victims up to 60% of the time - which is far more than the measly 15% that hooks regular Twitter phishing victims. The testing for this new automated tool focused on Twitter users who represent high value, such as those with a lot of followers or retweets. This helped keep the phishing attack out of the line of site of the Twitter defenses. Fortunately, the creators of this tool are the good guys. However, it's only a matter of time before the bad guys figure this out, too.

Tips and Advice

- It's always best to avoid clicking links in email messages or in other types of notifications, especially if they are not expected. Instead, go directly to the app or site using a previously bookmarked link or by typing the URL into the address bar. Be careful not to mistype it - this could lead to other infections by *typosquatters* or *do-jackers*.
- Use caution when clicking on videos or links from any social media site - even if they appear to have been posted by your friends. They may actually come from a hacker who has compromised your friend's account in some way. If you are suspicious in any way, it's best not to click it.
- If you click a link and it asks you if you want to run a program or execute something else, click the negative option unless you are 100% certain it's legitimate.
- Always keep your computers and mobile devices updated with the latest versions of software. Make one of those pieces of software a good anti-malware product.

The use of trademarks is not intended to endorse any company, product or service. Trademarks are the property of their registered owners.

Get the lastest information from our website. Scan the QR Code to go directly to this page.

© 2024 Bank of Utah
Equal Housing Lender NMLS #422914
Member FDIC